SHIELDX

SOLUTION BRIEF

APEIRO™ + Microsoft® Azure®

Protect your multi-cloud environments with comprehensive and uniform security policy

RightScale 2017 State of the Cloud Report: Among enterprises

have a multi-cloud strategy

clouds used + clouds tested

have adopted Azure

Azure

Compatible with
Microsoft Azure

Uncompromised Security

- Micro-segment and secure in minutes at scale
- Unlock traffic visibility
- Inspect and protect in depth with DPI
- Detect earlier via analytics and Indicator of Pivot (IoP)
- Protect more with uniform policy
- Align to risk and compliance

Unlimited Scale

- Scale-out and back-in elastically, up to multi-terabits of inspection
- Automate, insert and orchestrate
- Manage multi-cloud and multi-site
- Deploy over your infrastructure

Unparalleled Economics

- Save time with automation
- Empower DevOps with APIs
- Maintain SLAs with high availability
- Save costs with "lights off" removal
- Save your budget with cloud-friendly licensing at a fraction of the TCO and price

SECURING MULTI-CLOUD ENVIRONMENTS

Over the past years, cloud adoption among enterprises has steadily increased. While "private cloud adoption flattens" according to RightScale*, public clouds, and Microsoft Azure in particular, have gained traction, with Azure increasing adoption from 26% to 43% in 2016. This results in very diverse environments, with applications running across different public and private clouds, as well as in traditional data centers.

This multi-cloud landscape brings significant challenges with it, particularly when migrating workloads and securing them. Having to configure, for example, micro-segmentation policies for each of your distinct environments, is not feasible, especially keeping in mind the shortage of skilled security professionals.

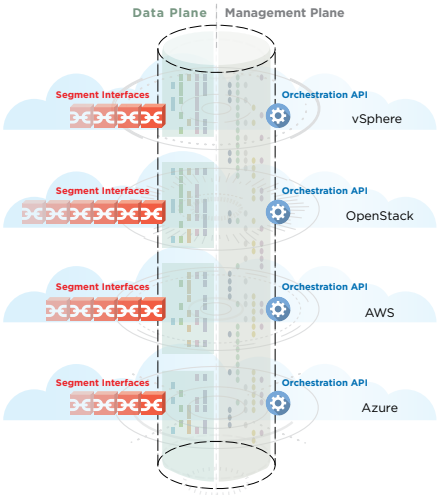
Thus, when evaluating security solutions for Azure or multi-cloud environments, IT teams are confronted with critical questions such as:

- Will this solution provide protection and compliance through intent-based, uniform, security policy in an automated fashion across lateral attack surfaces and multiple environments?
- Can this solution optimize our security resources and investments?
- Is it necessary to disruptively touch every workload to deploy? Will a host-based solution provide true isolation and network visibility?
- Does a network-based approach allow us to practically operationalize a virtual network security appliance in our Azure instances?

*RightScale 2017 – State of the Cloud Report

INTRODUCING APEIRO MULTI-CLOUD SECURITY

APEIRO is the first containerized, microservices platform for multi-cloud security. Natively software-defined and enabled by its uniquely distributed and elastic architecture, APEIRO provides deep packet inspection (DPI) and network-based security automatically and on-demand, across multiple environments, at logically unlimited scale.



Security Controls —Network-based and Full-Flow

- App-aware micro-segmentation
- Threat detection and prevention
- Malware detection
- TLS decryption and termination
- URL classification and filtering
- Data Loss Prevention (DLP)*
- Real-time event correlation
- Threat intel feed import*
- Data export

*Available in subsequent releases

Support

Our goal is to help enterprises maximize the value and benefits of their infrastructure automation, virtualization and security investments.

ShieldX Networks offers customers global, 7x24 technical support included with their subscription.

Contact Us
ShieldX Networks, Inc.
2025 Gateway Place, Suite 400
San Jose, CA 95110

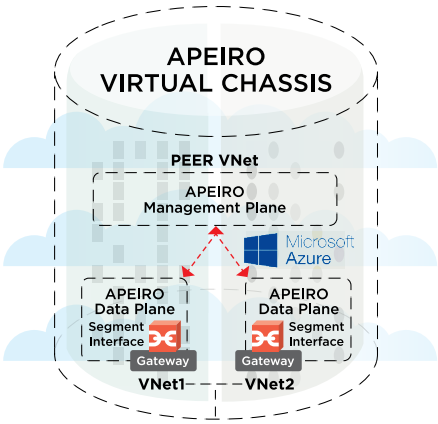
+1 408-758-9400
info@shieldx.com

www.shieldx.com

USING APEIRO TO SECURE AZURE ENVIRONMENTS

Advanced Security Orchestrated in Public Cloud in Minutes

Whether you start your APEIRO deployment in Azure or want to expand an existing deployment, securing your Azure environment takes only few mouse clicks. You log into your Azure account, navigate to the marketplace and instantiate one APEIRO image. From there you proceed to manage your deployment from within the APEIRO user interface by creating an infrastructure connector and a deployment specification. APEIRO will then automatically insert and, in alignment with your security, traffic and budget needs, scale in and out.



Each APEIRO Virtual Chassis has a single Management Plane, and one or more Data Planes. The Management Plane can manage across VNets and non-Azure environments and can be located within a peer VNet or in another connected environment.

Optimize Your Investments and Your Infrastructure

- Automatically collect and inspect traffic, even as your environment changes
- Uniform security policy enforced across all your environments, based on your intent
- Understand and visualize advanced attack behavior at all stages of the kill chain, including lateral movement
- Achieve both security and compliance with micro-segmentation implemented in a scalable fashion, with policy enforcement up through Layer 7
- Reduce both CAPEX and OPEX costs and consume fewer infrastructure resources

Requirements and Costs Over Your Azure Infrastructure

COMPATIBILITY

- Services: Azure

BASE CONFIGURATION (per license and traffic inspection rate)

MANAGEMENT PLANE (if Azure only)	SEGMENT INTERFACE, FLOW & INSPECTION	SSL/TLS DECRYPTION (Optional)
• 1 x DS13_V2 per 40Gbps inspection	• 2 x F4S Standard per 1Gbps inspected traffic	• 1x F8S Standard per 0.5Gbps encrypted inspection

LEARN MORE

Experience it now. Evaluate APEIRO with our proof-of-value program by contacting ShieldX or our authorized Partners through our website at www.shieldx.com.

© 2017 ShieldX Networks, Inc. All rights reserved. For trademark, copyright, patent, and other intellectual property and legal information, visit www.shieldx.com/legal